IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the application of :

| | | | |
|---|---|---|---|
| Appl. No. | : | 09/435,899 | Confirmation No. 5856 |
| Applicant | : | P. J. Seger | |
| Filed | : | 11/08/1999 | |
| TC/A.U. | : | 2175 | |
| Examiner | : | J. F. Betit | |
| Docket No. | : | TU999050US1 | |



Title: WIRELESS SECURITY ACCESS MANAGEMENT FOR A PORTABLE DATA STORAGE CARTRIDGE

**SECOND DECLARATION UNDER 37 C.F.R. Section 1.132**

I, Paul M. Greco, declare and say:

That I am a citizen of the United States of America and I reside at 2791 W. Woodview Crest Drive, Tucson, AZ 85742, USA.

That I am a Senior Programmer at IBM Systems Group, in the field of tape drive microcode development, since April 1996.

That I was previously a Senior Design Engineer at Environmental Systems Products, Inc., in the field of code and systems architecture and development, from August 1990 to April 1996.

That I attended college from 1987 to 1988 at the University of Arizona, located in Tucson, AZ.

That I am knowledgeable in the technology and science of Computer Science and Computer Engineering.

That I have reviewed the present U. S. Patent Application Serial No. 09/435,899, and find that it describes "a portable security system *** which resides in a portable data storage cartridge for managing access to the portable data storage cartridge". (Page 3, lines 13-16).

"A programmable computer processor is mounted in the portable data storage cartridge and coupled to [a] wireless interface. *** The computer processor provides a user table comprising at least one unique user identifier for each authorized user, *** and at least one permitted activity the user is authorized to conduct with respect to the data storage media. The user identifier, when combined with a user authentication message from the authorized user in accordance with a predetermined algorithm, authorizes the user." (Page 4, lines 2-14) (emphasis added).

"The computer processor *** receives user authentication messages from the data storage drive via the wireless interface and combines the user authentication message with the user identifier from the user table in accordance with the predetermined algorithm to authorize or deny the user activity". (Page 4, lines 15-21). The permitted activities may comprise management of access, for example, to "5) add entries to the user table, and 6) change/delete entries to the user table." (Page 5, lines 10-16).

That I have reviewed International Publication No. WO 87/07062, Anderl et al., and find that it relates to a "high security portable data carrier system ***" (Page 2, lines 7-8), with "an executive operating system that is accessed from the station via a set of *** command primitives" which "manipulate the card file system in accord with rules required by card security" (Page 2, lines 17-20).

"Security for the card is provided by requiring a separate password for gaining access to each of designated levels of interaction between the card and the associated station." (Page 2, lines 27-29) (emphasis added).

I) That, a fundamental distinguishing difference exists between the "designated levels of interaction" of Anderl et al. and the

present '899 Application's "at least one unique user identifier for each authorized user". (Page 4, lines 8-9) (emphasis added).

To base an argument on Anderl et al., regardless of the actual number of users, there would be only ONE user at any given access level, or login level. To equate "user" with "login level" requires that all "users" of a particular characteristic (in Anderl et al.) are indistinguishable. (see Anderl et al. Figures 2, 3 and 6, and Page 10, line 12 - Page 11, line 36).

In contrast, access characteristics are defined with respect to "each authorized user" in the present '899 Application.

In the present '899 Application, the access characteristics are part of the user table, allowing a many/many relationship where access privilege follows the user by means of the "user table comprising at least one unique user identifier for each authorized user". (Page 4, lines 8-9) (emphasis added).

II) That, Anderl et al. requires that a login specify the level and password as a specific request. (Page 11, lines 14-16).

In contrast, in the present '899 Application, access permissions of the user table are separate from the authentication method. The user table comprises "at least one unique user identifier for each authorized user, *** and at least one permitted activity the user is authorized to conduct with respect to the data storage media. The user identifier, when combined with a user authentication message from the authorized user in accordance with a predetermined algorithm, authorizes the user." (Page 4, lines 2-14) (emphasis added).

III) That, Anderl et al. relies on a fixed relationship between all login levels (i.e., the password may be changed for levels lower than the currently logged in level). (Page 11, lines 21-26).

In contrast, again, access characteristics are defined with respect to "each authorized user" in the present '899 Application.

In the present '899 Application, the access characteristics are part of the user table, allowing a many/many relationship where access privilege follows the user by means of the "user table comprising at least one unique user identifier for each authorized user". (Page 4, lines 7-9) (emphasis added).

That the undersigned declares further that all statements made herein of his own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patents issuing thereon.

Further declarant saith not.

Date: May 13, 2004 /s/ Paul M. Greco

Paul M. Greco